AF
IFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Assignee's Docket No.: 8490.00)
Group Art Unit: 2137)
Serial No.: 09/651,979)
Examiner: Michael Pyzocha)
Filing Date: August 31, 2000)
Title: Portable Terminal)

REPLY BRIEF

CERTIFICATE OF MAILING

I certify that this document is addressed to Mail Stop AF, Commissioner of Patents, PO Box 1450, Alexandria, VA 22313-1450, and will be deposited with the U.S. Postal Service, first class postage prepaid, on December 17, 2007.

Gregory A. Welte

SUMMARY OF A MAJOR POINT OF THIS REPLY

Claim 21(c) recites

1) encrypting a key K1,

2) transmitting the encrypted K1 to a terminal,

3) receiving an encrypted response from the terminal, and

4) de-crypting the response using the same key K1.

The Answer asserts that the first two items in this process are found in Yacobi, column 9, lines 44 - 54.

The Answer asserts that the last two items are found in column 10, lines 7 - 31.

However, Appellant submits that the Answer is incorrect in at least four respects.

One is that the wallet in Yacobi receives digital cash from the bank. But the bank did not encrypt that digital cash using K1. Yacobi expressly states that "the bank's private signing key" is used, not K1 (the key used by the wallet). (Column 10, lines 23 - 25.) Thus, K1 in the wallet cannot de-crypt the digital cash.

A second respect is the fact that Yacobi states that a "different pair of signing keys" is used "for each denomination" (such as one-dollar cash, five-dollar cash, etc.) (Column 10, lines 26, 27.) Thus, those "signing keys" cannot correspond to K1. At any given time, only a single K1 exists. So, even if the wallet did de-crypt the digital cash, the wallet can only de-crypt **a single denomination**. That is not a reasonable interpretation.

A third respect is that Yacobi does not state that the wallet de-crypts the digital cash. The Answer is interpreting Yacobi as teaching this, but has provided no evidence.

Further, Appellant submits that such de-cryption by the wallet makes no sense. If the owner of the wallet can de-crypt the digital cash, and thereby obtain plain text of the message representing the digital cash, then the owner can alter the cash amount. Nobody would allow that.

Instead, the merchant at which the wallet-owner spends the digital cash will perform the de-cryption.

As a fourth respect, Appellant points out that, if the wallet in Yacobi were to de-crypt the digital cash, then the wallet must be equipped with de-cryption keys which correspond to the "private signing keys" of the bank. (Column 10, lines 23 - 26.)

Yacobi mentions no such keys.

And finally, Appellant submits that equipping the wallet with such keys makes no sense. That means that the wallet owner would be in possession of (1) an encrypted message (the digital cash) and (2) keys to de-crypt the message.

That is an invitation for the wallet owner to fabricate his own digital cash.

END SUMMARY

REPLY TO EXAMINER'S ANSWER ("ANSWER" HEREIN), PAGES 6 - 7

Issue 1

The Answer's contentions are based on a false premise, namely, that the symmetric key K1 in Yacobi is used by the bank to "digitally sign" the hash value. (See column 10, line 23 et seq.)

As background, Appellant points out that a symmetric key K1 is effective to both **EN**crypt a message, and then **De**-crypt the message which K1 was used to encrypt. This can be illustrated graphically:

K1
PLAIN TEXT --->>> CYPHER TEXT

This means that K1 is used to **EN**crypt the PLAIN TEXT into CYPHER TEXT.

K1
CYPHER TEXT --->>> PLAIN TEXT

This means that **the same key K1** can recover, by **DE-crypting,** the plain text from the cypher text.

But this operation does not occur in the passages in Yacobi, which are cited by the Answer.

In those passages, Yacobi encrypts data being transmitted from the "electronic wallet" to a bank's computer, using K1, which he calls a "session key." (Column 9, lines 44 - 49.)

The bank then returns a "hash" (ie, hash value) of data which represents money. Yacobi may state that the "hash" is encrypted, because he states that it is "digitally signed." (Column 10, lines 22, 23.)

But nowhere does Yacobi state that key K1 is used to encrypt that "hash." The Answer's assertions are simply incorrect.

Further, several points about Yacobi in this context should be noted.

Point 1

The Answer seems to be implying that the presence of a "session" key implies that all encryption in a given transaction, or session, is done using that key. Appellant points out that a "session" key does not imply that.

A "session" key is one which is used for a given operation, or set of operations, and then discarded. A "session" key is a disposable key.

It is not necessarily used for every operation in a group of operations.

Point 2

The Answer's contention is **directly rebutted** by Yacobi himself. The Answer asserts that encryption of the "hash" by the bank is done using K1.

Appellant points out that, if any encryption is done of the "hash," that encryption is found in the "digitally signing" of Yacobi's column 10, line 23.

But Yacobi **expressly states** that he uses a **"different pair of signing keys for each denomination"**. (Column 10, lines 26, 27; "denominations" refers to the values of the digital cash: one dollar, five dollars, etc.)

Thus, Yacobi's bank **cannot possibly** use K1 to encrypt the "hash." The key used depends on the "denomination" to which the key is applied, so different keys must be used for different denominations.

Point 3

Yacobi **expressly states** that the "hash" sent by the bank to the wallet **is not encrypted using K1.**

He states that the "session key" is used to encrypt data which is sent to the bank by the wallet. He also states that the "session key" itself is encrypted by the wallet. Both items (the encrypted data and the encrypted session key) are transmitted to the bank.

If the bank can de-crypt the encrypted session key, it can thus de-crypt the data, which it does. (Column 9, lines 47 - 57.)

But the "session key" has served its function, and is now destroyed by the bank. (Column 9, line 65 - column 10, line 1.)

Therefore, the "session key" is not used to encrypt anything further. The "hash" transmitted by the bank is encrypted using another key.

Issue 2

The Answer asserts that the digital cash, which was received by the wallet, "must be **DE**-crypted by the wallet." (Answer, top of page 7, emphasis supplied.)

Point 1

However, the Answer provides no authority for this assertion. Yacobi does not state that the wallet performs this de-cryption.

Since Yacobi does not discuss this de-cryption, the Answer is relying on the Doctrine of Inherencey. MPEP § 2112 states:

> EXAMINER MUST PROVIDE RATIONALE OR EVIDENCE TENDING TO SHOW INHERENCY.
>
> In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic <u>necessarily</u> flows from the teaching of the applied prior art.

The Answer has provided no "basis in fact and/or technical reasoning" explaining why the wallet would de-crypt the "hash."

Point 2

Such de-cryption would defeat the purpose of using digital cash. The "digital signing" of the digital cash by the bank allows the merchant, who receives the digital cash from the "wallet," to verify that the digital cash is genuine.

The customer, who owns the wallet, carries the digital cash to the merchant. But the customer cannot be given access to the digital cash, because the customer can then tamper with the amounts of digital cash.

A simple example will illustrate.

EXAMPLE

The digital cash is, in essence, a message. Consider this message:

THIS IS AN IMPORTANT MESSAGE.

In the computer world, each character in the message is represented by a number, such as its ASCII value. If spaces and punctuation are included, then this message contains 29 numbers.

Those numbers are applied as input to an algorithm, which produces an output, which is also a number. A simple algorithm would merely add all the numbers together, to form a sum. Of course, more complex algorithms are used in practice.

Suppose the output is 456. The plain text of the digital cash (ie, the message) is encrypted, and the number 456 (the output) is included in the message.

When the bank receives the encrypted message, it runs it through the same algorithm. If the number 456 is produced, then the bank assumes that the message has not been tampered with.

However, if the digital wallet **DE**-crypts the message into plain text, then this authentication process is completely defeated. The merchant has no way of knowing whether the wallet's owner has tampered with the message.

Therefore, common sense dictates that Yacobi's wallet does not de-crypt the digital cash.

Point 3

Even if the Answer is correct, and the wallet does de-crypt the digital cash (which Yacobi does not state,) the wallet **cannot use K1 for this process.**

The reason was explained above. The bank uses **different keys** (called "signing keys") to encrypt the digital cash. (Column 10, lines 26, 27.) Those "signing keys" are different from K1.

Further, as also explained above, **different** "signing keys" are used for "different denominations." That conclusively proves that K1 is not used to de-crypt the "hash."

REPLY TO ANSWER, PAGE 7, PASSAGE BEGINNING "In response to . . . POINT 1 . . ."

This passage directly contradicts the Answer's assertion that K1 is used to de-crypt the "hash."

This passage states that "the hash value is signed by encrypting it with the bank's private key."

If that be so, then how does K1, in the wallet, de-crypt something which was encrypted using "the bank's private key" ?

REPLY TO ANSWER, PAGE 7, PASSAGE BEGINNING "In response to . . . POINT 2 . . ."

In the Answer's scenario, the **merchant** performs the de-crypting. The "wallet" in Yacobi does not.

The merchant's de-crypting does not correspond to the claim language.

REPLY TO ANSWER, PAGE 8, PASSAGE BEGINNING "In response to . . . POINT 4 . . ."

This passage has been addressed above.

This passage repeats the assertion that the wallet de-crypts the "hash." This assertion has been addressed above.

REPLY TO ANSWER, PAGE 8, PASSAGE BEGINNING "In response to . . . POINT 5 . . ."

This passage fails to rebut the Brief. This passage arbitrarily asserts that Yacobi's wallet de-crypts the "hash." This arbitrary assertion has been addressed herein.

REPLY TO ANSWER, PAGE 9, PASSAGE BEGINNING "With respect to . . ."

The Answer asserts that it is substituting one equivalent for another. MPEP § 2144.06 states:

> In order to rely on equivalence as a rationale supporting an obviousness rejection, **the equivalency must be recognized in the prior art**, and cannot be based on . . . the mere

> fact that the components at issue are functional or mechanical equivalents.

The Answer has failed to show that the equivalency is recognized in the prior art, as required.

Further, as the Brief explains, page 43, "Problem 2," Menezes discusses **numerous** approaches to generating a seed. Those other approaches do not show the claimed subject matter.

REPLY TO ANSWER, PAGE 9, PASSAGE BEGINNING "In response to . . ."

Point 1

This passage fails to rebut the Brief.

Point 2

The Brief pointed out that both references impliedly state that they want random keys, or seeds, because that is a recognized goal in the science of cryptography. Thus, as a matter of logic, there is no reason to combine the references to pursue that goal (of a random seed), because nothing new is obtained.

Point 3

This passage implies that the references are deficient because their keys should be random, but are not. Then the passage asserts that pursuit of true randomness is a valid motivation.

But this motivation leads nowhere. The Answer has not shown how the goal of true randomness is obtained.

Until that is shown, the motivation is not actually motivation, but is actually a **wish**.

Until the Answer shows how this **wish** is fulfilled by the combined references, the motivation of seeking true randomness is not a basis for combining the references.

The reason is that the combined references do not produce true randomness (or at least this has not been shown).

Point 4

From another perspective, the motivation is logically irrelevant to combining the references, and thus does not promote the combination. The motivation sets forth a goal (or wish), which the references, even if combined, do not attain.

Point 5

This passage actually makes no sense, when read literally. It states "[A] key should be random, but the mere use of a key does not mean it is inherently random."

If you strip out the excess verbiage, this statement means "A key should be random, but it is not random."

Appellant asks, "What is the point ?"

Point 6

No expectation of success has been shown, indicating that the combination of references actually produces a truly random key.

MPEP § 706.02(j) states:

> Contents of a 35 U.S.C. 103 Rejection
>
> . . .
>
> To establish a prima facie case of obviousness, three basic criteria must be met.
>
> . . .
>
> Second, there must be a reasonable expectation of success.
>
> . . .
>
> The . . . reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure.

REPLY TO ANSWER, PAGE 10, PASSAGE BEGINNING "In response to . . . Problem 2 . . ."

The Answer asserts that it can arbitrarily select one teaching in a reference, and ignore others.

MPEP § 2141.03, last paragraph, states:

> Prior art must be considered in its entirety, including disclosures that teach away from the claims.

MPEP § 2111 states:

> PRIOR ART MUST BE CONSIDERED IN ITS ENTIRETY,

> INCLUDING DISCLOSURES THAT TEACH AWAY FROM THE CLAIMS
>
> A prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention.

Therefore, the Answer's assertion that it can cite references for particular purposes, and ignore contrary teachings, is not supported by the MPEP.

REPLY TO ANSWER, PAGE 10,
PASSAGE BEGINNING "In response to . . . Problem 3 . . ."

Point 1

The Answer's assertion that Menezes fails to teach **where** values should be stored does not rebut the Brief. (The values produce the seed.)

The Brief points out that Menezes states that the values should be hidden from adversaries. The Brief, page 44, states:

> Therefore, Menezes teaches against the recitation of claim 21 regarding user-accessibility to the records used for the seed. The Office Action has provided no rationale which overcomes Menezes' contrary teaching.

It appears that the Answer is asserting that Menezes fails to explain **where** the values are stored, so that, therefore, he teaches that the values should be available to a user, as the claims state.

Such an assertion fails as a matter of logic, particularly since Menezes **expressly states** that the "values" should be concealed.

Point 2

The Brief states:

> But Menezes' section 5.2 also states, "The generator must not be subject to observation."

The Answer states: "Menezes does not explicitly state this."

Appellant points out that Appellant made a **direct quote** of Menezes, yet the Answer asserts that Menezes did not make the quoted statement.

Appellant requests that the Board read section 5.2 of Menezes, and decide which to believe, the Answer or the Brief.

Point 3

The Answer states "Therefore, Menezes does not teach away from storing the records in user-accessible memory."

Appellant points out that this assertion focuses on the wrong issue, and in the wrong context.

The invention is concerned with using non-secure "records" to form a seed.

The question is whether Menezes teaches that accessible records should be used to form a seed.

REPLY TO ANSWER, PAGE 11, PASSAGE BEGINNING "Appellant Argues . . ."

This passage fails to rebut the Brief.

It is not known which of the two approaches outlined in the Brief are used by Menezes.

The Answer is asserting that observation, as in the Brief's example, amounts to "storage." If so, Appellant then asks, "How are the observed values then later recovered ?"

If they were "stored" by writing them down, or by loading into memory, then they could be recovered. But if they were observed and then inserted into an algorithm, and not individually recorded, that does not amount to "storage," as claimed.

An analogy seems appropriate. Suppose I want to generate a random number. My approach is to put a weather vane on my roof, and a wind speed indicator (anemometer). At any given time,

-- the weather vane will point in one of 360 directions, for a value from 1 to 360,

-- the anemometer will read a value between 0 and 100 mph. (It breaks at 101 mph.)

My random number is the sum of the two values. I take a reading every ten seconds. And I add each pair of readings to the preceding pair, making a running total.

Have I "stored" the values ? No. I cannot recover the individual values.

Appellant points out that the claim term must be applied consistently with the Specification. For example, claim 21(a) states that the "records" are stored in "user-accessible memory." Claim 21(b) states that the "seed" for key K1 is generated from those "records."

Thus, the "records" must be retrievable.

In one of the approaches of Menezes, the stored data is not retrievable. Thus, that approach does not produce the claimed invention.

The Answer has provided no teaching for selecting another approach in Menezes, to the exclusion of the non-storage approach. The Answer has not shown the claimed invention in the references.

REPLY TO ANSWER, PAGE 11,
PASSAGE BEGINNING "In response to . . . Problem 5 . . ."

The Answer is invoking completely arbitrary principles. It has given no valid reason for selecting the software method over the hardware method.

This is proven by the fact that the reasons stated are utterly non-specific. That is, if the Answer wanted to select the other method, the hardware method, the same basic reasons could be used.

Thus, the reasons set forth by the Answer do not, in fact, militate in favor of selecting one approach over the other in Menezes.

REPLY TO ANSWER, PAGE 12,
PASSAGE BEGINNING "In response to . . . Problem 6 . . ."

The Answer has admitted that it is using the claims as a check-list for selecting and combining elements in the prior art.

That is not allowed, and is specifically prohibited by the MPEP. MPEP § 706.02(j) states:

> Contents of a 35 U.S.C. 103 Rejection
>
> . . . After indicating that the rejection is under 35 U.S.C. 103, the examiner should set forth in the Office action:
>
> (A) the relevant teachings of the prior art relied upon, preferably with reference to the relevant column or page number(s) and line number(s) where appropriate,
>
> (B) the difference or differences in the claim over the applied reference(s),
>
> (C) the proposed modification of the applied reference(s) necessary to arrive at the claimed subject matter, and
>
> (D) an explanation why one of ordinary skill in the art at the time the invention was made would have been motivated to make the proposed modification.
>
> To establish a prima facie case of obviousness, three basic criteria must be met.
>
> First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally

> available to one of ordinary skill in the art, to modify the reference or to combine reference teachings.
>
> Second, there must be a reasonable expectation of success.
>
> Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.
>
> **The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure.**

Further, MPEP § 901.03 states:

> Pending Applications
>
> . . . pending U.S. applications are preserved in confidence (37 CFR 1.14(a)) and are not available as references.

Since the Appellant's application is not available as a reference, it cannot be used as a teaching for selecting one part of a reference over another.

REPLY TO ANSWER, PAGE 12, PASSAGE HEADED "Claims 22 and 23"

No reply is needed.

REPLY TO ANSWER, PAGE 12, PASSAGE HEADED "Claim 24"

No reply is needed.

Appellant points out that the Answer asserts that Appellant's arguments are "moot" in view of the Answer's response. But "moot" means "deprived of practical significance" or "rendered irrelevant."

The Answer's response has not caused Appellant's arguments to become devoid of significance, or irrelevant. At best (for the Answer), Appellant's arguments are rebutted by the Answer. But that does not render Appellant's arguments "moot."

This response applies to the Answer's other assertions of mootness.

REPLY TO ANSWER, PAGE 13, PASSAGE HEADED "Claim 26"

No reply is needed.

REPLY TO ANSWER, PAGE 13, PASSAGE HEADED "Claim 27"

Point 1

Claim 27 depends from claim 26. Claim 27 recites two keys, named EM2 and K2.

The Brief points out that EM2 and K2 have not been shown in the references. The Answer fails to cure this defect.

Point 2

The Answer asserts that the digital cash is de-crypted by Yacobi's wallet. As explained above, Yacobi does not say that, and that would defeat the purpose of digital cash.

Further, Appellant asks a practical question: "What purpose would be served by Yacobi's de-crypting of the digital cash in the wallet ?"

Point 3

The Answer asserts that the bank encrypts the digital cash using the session key, K2 in this example.

Appellant pointed out above that this is not so. Yacobi states that the key used depends on the "denomination," and expressly states that a different key is used than that asserted by the Answer.

REPLY TO ANSWER, PAGE 14, PASSAGE HEADED "Claims 28 and 30"

Background

Claim 28 states that a PDA "has no secure area." Thus, a user can gain access.

Yacobi states that his device is "tamper resistant."

Yacobi is plainly contradictory to the claim language.

Reply

The Answer asserts that Yacobi is "tamper resistant" for one purpose (reverse engineering), yet **NOT** "tamper resistant" for another purpose (user access to memory, for example).

Several problems exist in the Answer's assertion.

Problem 1

The Answer's assertion is simply incorrect. The passage of Yacobi which the Answer cites states that **one purpose** of making a wallet "tamper proof" is to prevent reverse engineering.

But another purpose is to prevent "double spending" by modifying or cloning the wallet.

Problem 2

The Answer is looking at the **wrong wallet** in Yacobi.

The Answer is looking at a wallet in Yacobi's prior art, which Yacobi criticizes for its shortcomings.

The "tamper proof" wallet which Appellant pointed to is in column 5, lines 18, 19. That passage refers to a "wallet" which is "tamper resistant." Immediately after that passage, Yacobi discusses the "memory" which stores "assets" (eg, digital cash) and keys.

Further, as explained above, the owner of the wallet cannot be granted access to the "assets," ie, the digital cash.

Therefore, it is reasonable to conclude that the owner of the "tamper resistant" wallet in Yacobi does not obtain access to the "memory" which stores the "assets" and keys.

That is contrary to the claim.

Problem 3

The Answer is attributing an assertion to Yacobi which Yacobi does not actually make. That assertion is that Yacobi's wallet is "tamper-proof" for one purpose, but not for another.

Thus, the Answer is relying on the Doctrine of Inherency. As explained above, the PTO must provide an explanation showing why Yacobi should be interpreted in this manner.

Appellant submits that this is particularly true, since the Answer's assertion seems to make no sense. How, in practice, can something be "tamper proof" for one purpose, and not another ?

Further, why would Yacobi want the non-tamper-proof aspect to be present ? That is, it would seem that extra effort would be required to make the wallet both tamper proof (for one purpose) and **NOT** tamper proof (for another purpose).

If the wallet is made tamper proof for one purpose (as by manufacturing it in a stout locked case), then why not make it tamper proof all around ? That seems to make good engineering sense.

Problem 4

The Answer's conclusion is that the user memory in Yacobi is not secure. Again, Yacobi does not state this, and the Answer is relying on the Doctrine of Inherency. An explanation is required.

Problem 5

The last full sentence on page 14 of the Answer (beginning "Additionally . . .") contradicts the Answer's conclusions.

In that sentence, the Answer asserts that Yacobi's device requires a **higher** degree of security (in being "tamper proof" and not merely "tamper resistant").

That is contrary to the Answer's assertion that Yacobi's memory is available for tampering.

That is contrary to the Answer's assertion that Yacobi's wallet is tamper resistant only for some purposes.

Further, that sentence is directly contradicted by Yacobi, column 2, line 15 et seq., which states that a wallet can **NEVER** be made "tamper proof."

REPLY TO ANSWER, PAGE 15, PASSAGE HEADED "Claims 32, 33, and 38"

No reply needed.

REPLY TO ANSWER, PAGE 15, PASSAGE HEADED "Rejection of Claims . . ."

Point 1

The Answer asserts that the claims are ambiguous, in failing to state where the PIN is entered.

Appellant points out that the Answer is incorrect.

Claim 35 recites:

> wherein **the portable computer requires entry of a Personal Identification Number, PIN**, prior to generation of the encryption key, and will not complete the transaction without the PIN.

This claim states that the PIN must be entered into the "portable computer."

This applies to claims 36 and 37.

Point 2

The Answer further asserts that, even if the claims require entry of the PIN into the portable computer, the reference shows that, because the PIN is pre-stored in the reference, and must have been entered previously, for that storage.

Appellant points out that this interpretation relies on the wrong PIN, entered at the wrong time. The events cited in the reference, and relied on by the Answer, do not correspond to the claim recitations.

For example, parent claim 21 recites a process, and dependent claim 35 recites a PIN, and a relationship to that process.

The events cited in the reference do not correspond to the claim recitations. For example, when the PIN is pre-entered in the reference, no process as in claim 21 exists.

Re: "Problem 1," Page 16 of Answer

The Answer was addressed above.

Re: "Problem 2," Page 16 of Answer

The PTO must show a teaching for

1) verifying the customer at the portable computer (as opposed to verifying at the nearby ATM)

and

2) performing the verification at the portable computer using a PIN (as opposed to fingerprint recognition, for example).

That has not been done.

The Answer merely asserts that the PIN is one way of identifying a person.

Appellant points out that this type of reasoning is not allowed by the MPEP. MPEP § 2143.01 states:

> FACT THAT REFERENCES **CAN BE COMBINED** OR MODIFIED IS NOT SUFFICIENT TO ESTABLISH PRIMA FACIE OBVIOUSNESS
>
> The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination.
>
> . . .

> FACT THAT THE CLAIMED INVENTION IS **WITHIN THE CAPABILITIES OF ONE OF ORDINARY SKILL IN THE ART** IS NOT SUFFICIENT BY ITSELF TO ESTABLISH PRIMA FACIE OBVIOUSNESS
>
> A statement that modifications of the prior art to meet the claimed invention would have been "well within the ordinary skill of the art at the time the claimed invention was made" because the references relied upon teach that all aspects of the claimed invention were individually known in the art is not sufficient to establish a prima facie case of obviousness without some objective reason to combine the teachings of the references.

The Answer is, in essence, making the type of rejection prohibited by this MPEP section.

Re: "Problem 3," Page 17 of Answer

Point 1

Appellant repeats a passage from the Brief.

> Yacobi discusses an ATM. (Column 5, line 35.) Everybody knows that ATMs require PINs to be entered onto the ATM's keypad. Thus, Yacobi teaches entering a PIN onto an ATM keypad.
>
> (Brief, page 55.)

Point 2

The Answer asserts that Yacobi implies entry of a PIN into his wallet. Since Yacobi does not actually state this, the Answer is relying on the Doctrine of Inherency. An explanation is required as to why Yacobi should be so interpreted.

Point 3

The Answer asserts that "Yacobi never discloses the use of a PIN for user verification."

Appellant points out that Yacobi states that he verifies the user of an ATM "using traditional methods." (Column 9, lines 16 - 18.)

Plainly, "traditional methods" imply requesting a PIN be entered into the ATM.

The undersigned attorney started using ATMs around 1985. If he used an ATM once per week, then he has used an ATM 52 times per year, for more than 20 years, for a total of over 1,000 usages.

He entered a PIN every time.

The Answer's interpretation of Yacobi in this respect is not plausible.

CONCLUSION

Appellant requests that the Board overturn the rejections, and pass all claims to issue.

Respectfully submitted,

Gregory A. Welte
Reg. No. 30,434

NCR Corporation
1700 South Patterson Blvd.
WHQ - 4
Dayton, OH 45479
December 17, 2007
(937) 445 - 4956